# БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

ФИО преподавателя: Селин А.А., канд. техн. наук

# ОРГАНИЗАЦИЯ ЗАЩИТЫ ДАННЫХ В СООТВЕСТВИЕ С КОНЦЕПЦИЕЙ БЕЛЛА – ЛАПАДУЛЫ

Учебные вопросы:

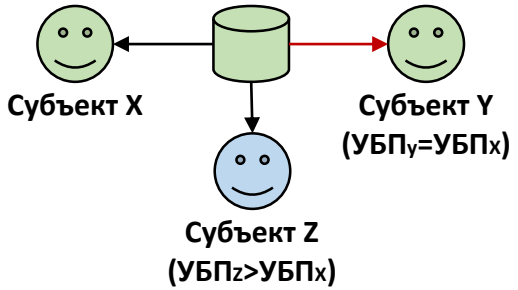
1. Каналы утечки в системах с дискреционной моделью доступа
2. Модель защиты данных Белла – Лападулы на основе мандатов
3. Организация защиты базы данных

# КАНАЛЫ УТЕЧКИ В СИСТЕМАХ С ДИСКРЕЦИОННОЙ МОДЕЛЬЮ ДОСТУПА

**Основные недостатки дискреционной модели доступа (концепция подсхем пользователей):**

Если субъект X получил доступ в соответствие со своим уровнем благонадежности пользователя к данным с некоторой степенью конфиденциальности, то ему ничто не помешает передать эти данные субъекту Y с более низким уровнем благонадежности.


Не обеспечивается монопольное владение данными их владельцу. Если субъект X имеет уровень благонадежности, такой же, как и у субъекта Y, то его данные полностью доступны и субъекту Y, а также всем субъектам с более высоким уровнем благонадежности.



# КАНАЛЫ УТЕЧКИ В СИСТЕМАХ С ДИСКРЕЦИОННОЙ МОДЕЛЬЮ ДОСТУПА

**Основные недостатки дискреционной модели доступа (концепция подсхем пользователей):**

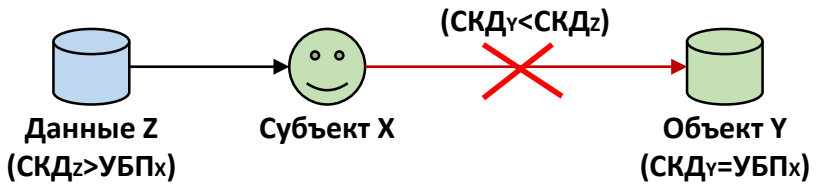
Концепция требует распределения данных разной степени конфиденциальности по изолированным хранилищам. Следовательно субъект X с уровнем благонадежности, допускающем его к данным с несколькими степенями конфиденциальности, вынужден смешивать информацию из разных классов конфиденциальности.


Смешение данных с разными степенями конфиденциальности в одном контейнере (документе, изделии) приводит к необходимости завышения класса конфиденциальности (по наивысшей степени) данных, которые не содержат тайну (с низкой степенью конфиденциальности).

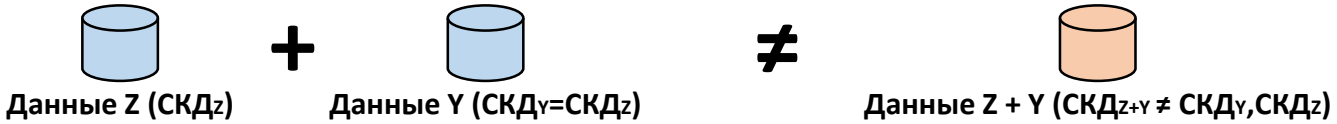
# КАНАЛЫ УТЕЧКИ В СИСТЕМАХ С ДИСКРЕЦИОННОЙ МОДЕЛЬЮ ДОСТУПА

**Основные недостатки дискреционной модели доступа (концепция подсхем пользователей):**

Ставшие известными субъекту X частные данные со степенью конфиденциальности, превышающей его уровень благонадежности, не могут быть помещены им в недоступное ему информационное хранилище.



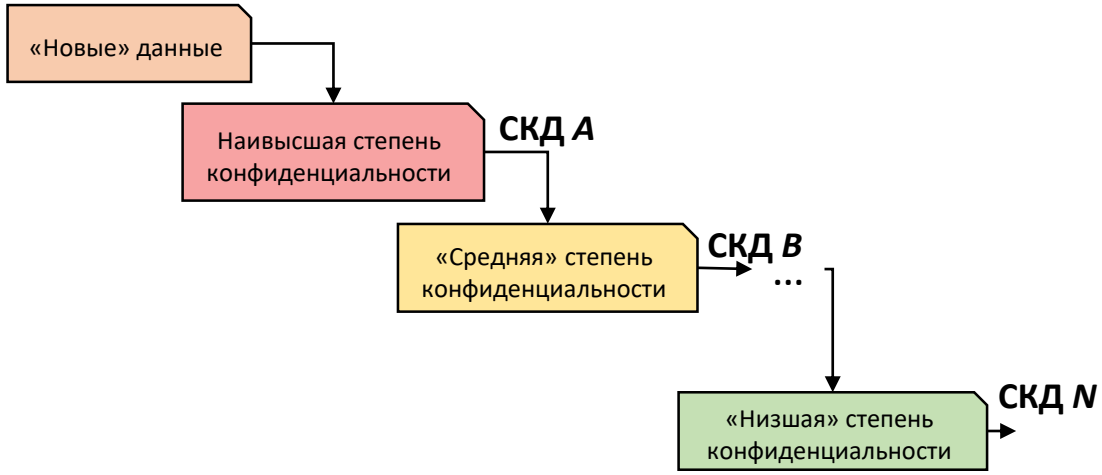

Концепция не позволяет изменить степень конфиденциальности данных «по совокупности сведений», если такая необходимость возникнет.



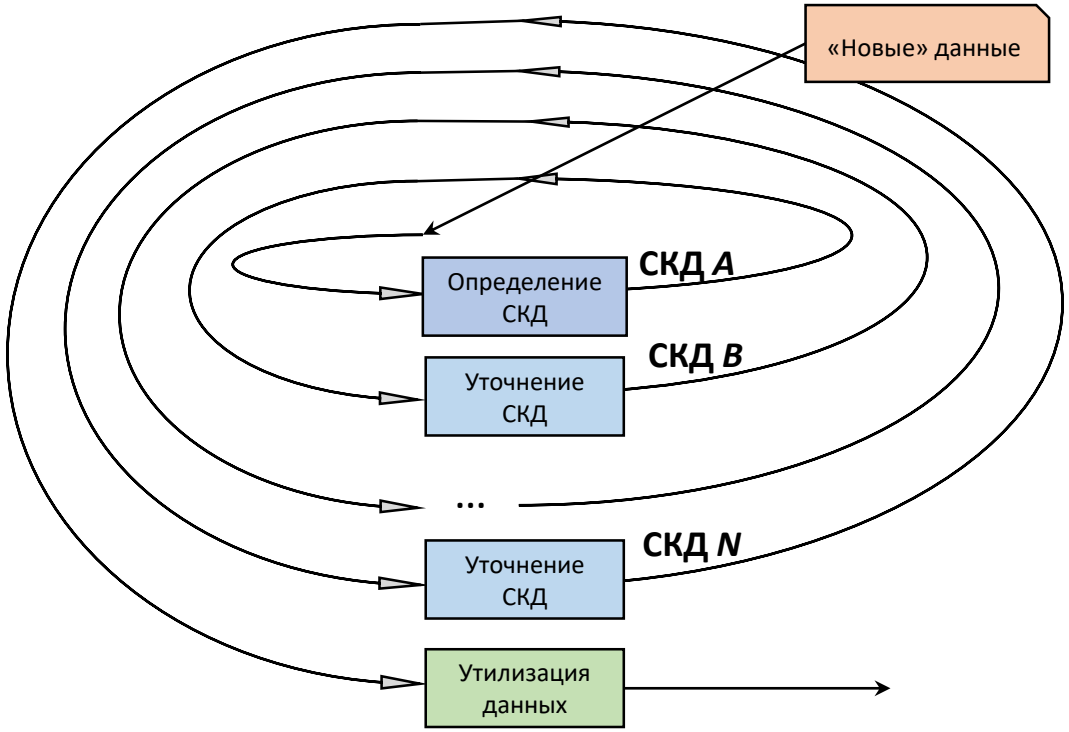
# МОДЕЛЬ ЗАЩИТЫ ДАННЫХ БЕЛЛА – ЛАПАДУЛЫ НА ОСНОВЕ МАНДАТОВ

## Жизненный цикл конфиденциальной информации

### Каскадная модель жизненного цикла конфиденциальной информации

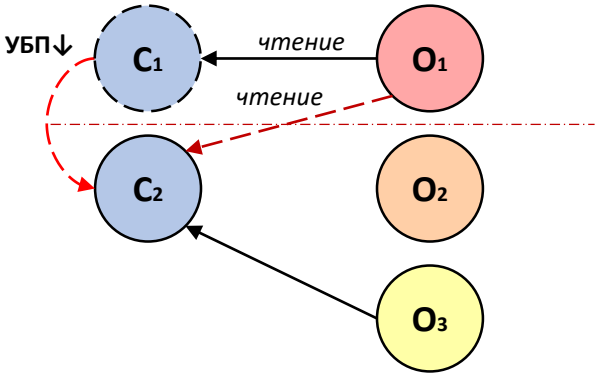



### Спиральная модель жизненного цикла конфиденциальной информации



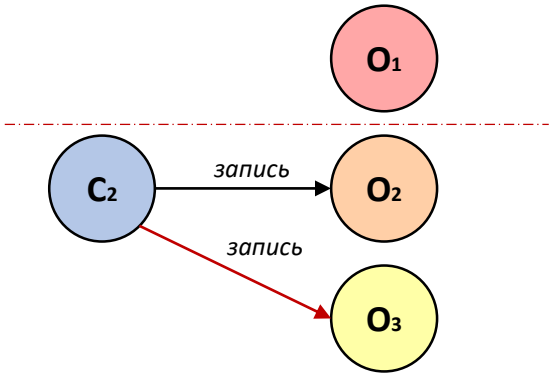
# МОДЕЛЬ ЗАЩИТЫ ДАННЫХ БЕЛЛА – ЛАПАДУЛЫ НА ОСНОВЕ МАНДАТОВ

**Управление (изменение) степени конфиденциальности данных или уровня благонадежности пользователя**



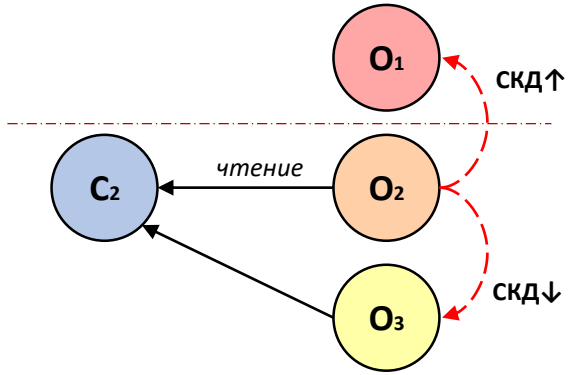

*Прецендент «памяти» ранее прочитанных данных с более высокой СКД*

Решение: запретить субъекту читать данные с СКД, более высоким, чем УБП субъекта




*Прецендент записи данных с более высокой СКД, чем у объекта базы данных*

Решение: запретить запись данных с СКД, более низким, чем УБП субъекта




*Прецендент предварительного чтения данных с более высокой СКД*

Решение: запретить чтение данных до определения их СКД

**Свойства безопасности модели Белла – Лападулы**

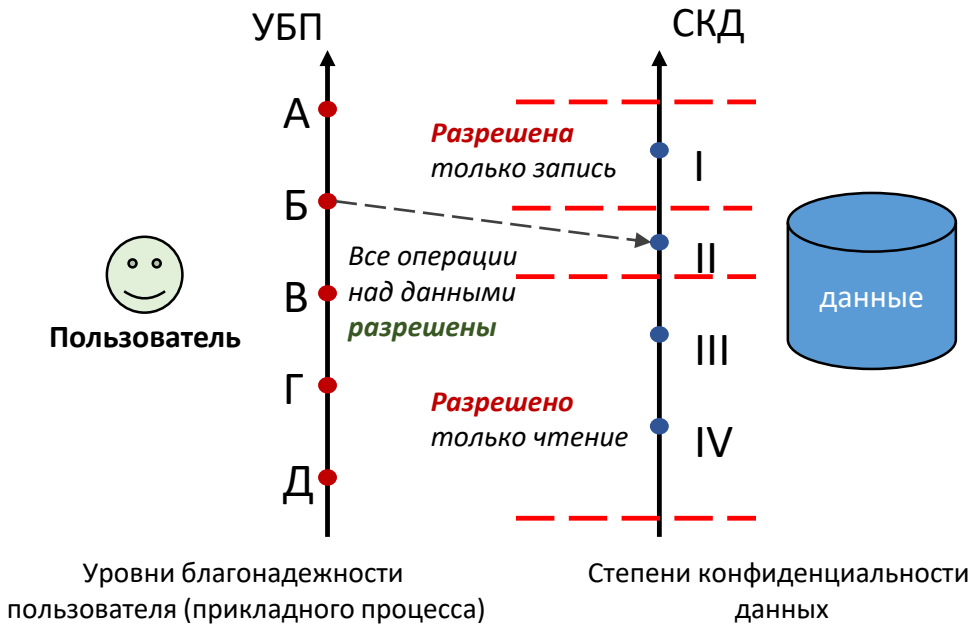
**[Простое свойство]** *Запретить субъекту читать данные, если их СКД выше, чем его УБП.*

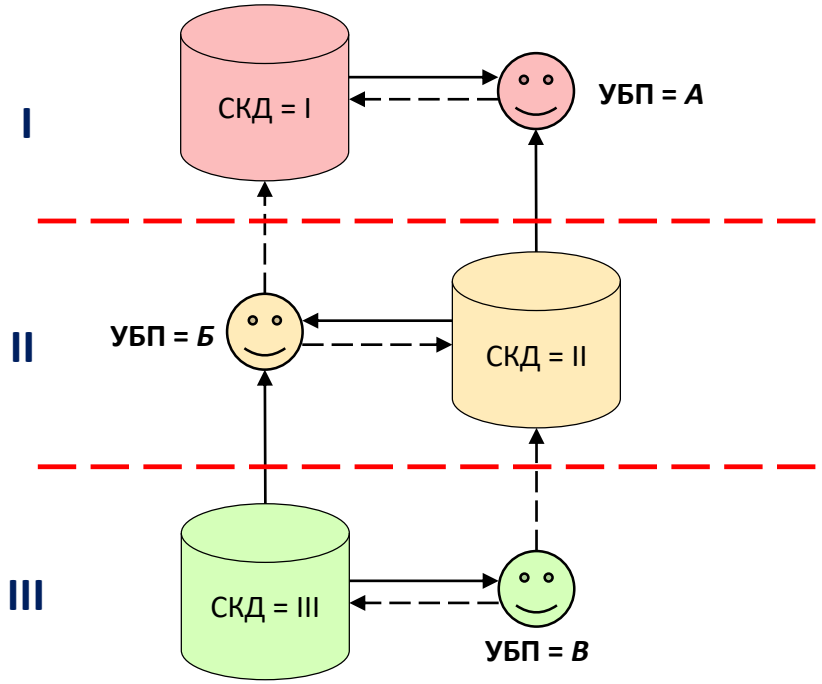
**[*- свойство]** *Запретить субъекту записывать данные, если их СКД ниже, чем его УБП.*

**[Дискреционное свойство]** *Субъекту разрешено и читать и записывать данные, только если его УБП совпадает с их СКД.*

# МОДЕЛЬ ЗАЩИТЫ ДАННЫХ БЕЛЛА – ЛАПАДУЛЫ НА ОСНОВЕ МАНДАТОВ

**Конечный автомат подсистемы защиты данных**




Все информационные потоки направлены «вверх» и в рамках уровня благонадежности / степени конфиденциальности. Следовательно, утечка конфиденциальных данных «вниз» не возможна.

# МОДЕЛЬ ЗАЩИТЫ ДАННЫХ БЕЛЛА – ЛАПАДУЛЫ НА ОСНОВЕ МАНДАТОВ

**Матрица безопасности базы данных, защищенной в соответствие с концепцией Белла – Лападулы**

**МАТРИЦА БЕЗОПАСНОСТИ**

*Объекты защиты: столбцы, индексы, функции,..*

*Субъекты обработки: Роли / Учетные записи*

| | Table_A | Table_B.Attribute 1 | View_V | Index_I | … | Sequence_1 |
|---|---|---|---|---|---|---|
| User_1 | S | S, I, U, D | S | S | | I, U, D |
| User_2 | S | S | S | I, U, D | | S, I, U, D |
| User_3 | I, U, D | I, U, D | S | S | | S |
| … | | | | | | |
| User_X | S | S | S | I, U, D | | S |

*Привилегии*

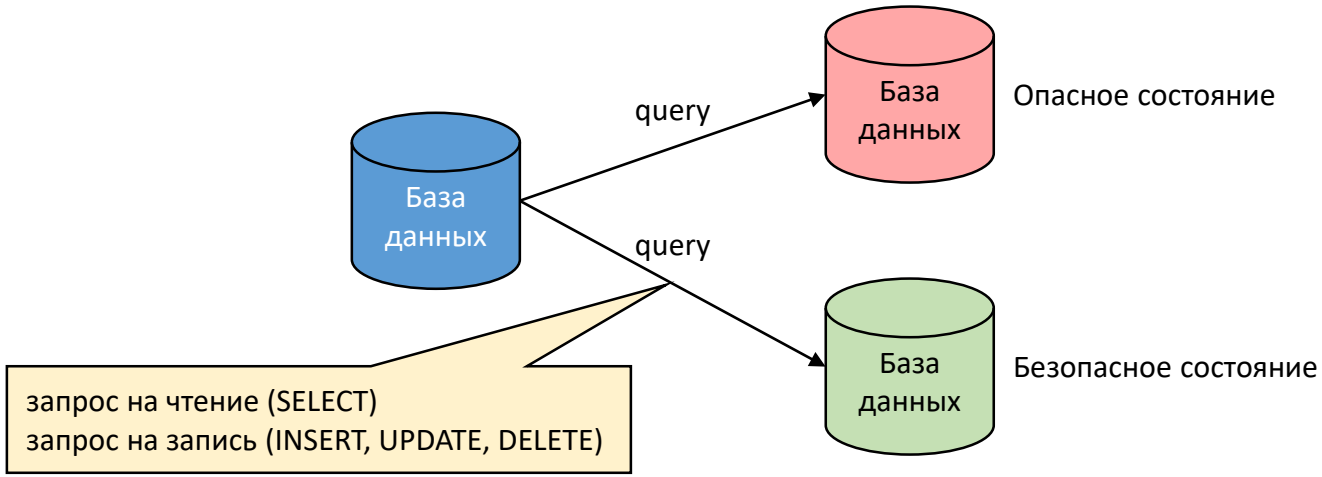
Принцип «запись вверх» (“no read up”)

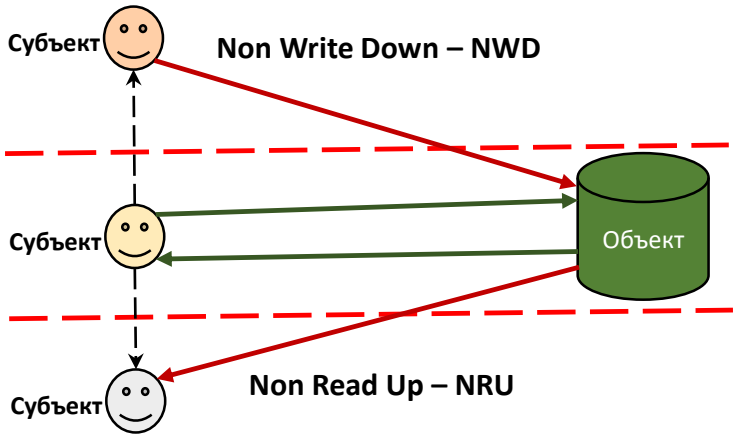
Полный доступ (СКД = УБП)

Принцип «чтение вниз» (“no write down”)

Матрица безопасности не имеет ячеек со значением NULL.
Каждая ячейка является мандатом на доступ к минимальной порции данных.
Каждая ячейка физически реализуется SQL-предложением GRANT.
Число SQL-предложений должно быть равно числу ячеек матрицы.

# ОРГАНИЗАЦИЯ ЗАЩИТЫ БАЗЫ ДАННЫХ



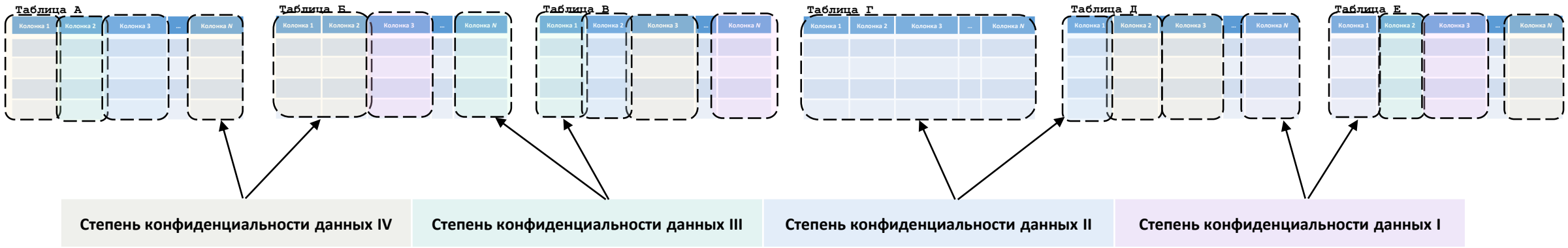

**Теорема Белла – Лападулы:**

1. Начальное состояние БД – безопасно.
2. Функция переходов БД в новое состояние под воздействием запроса (query) должна обеспечивать гарантированное достижение безопасного состояния:

а) если входной запрос на чтение, то он выполняется только когда УБП субъекта не ниже СКД читаемых данных;
б) если входной запрос направлен на чтение данных с СКД, превышающем УБП субъекта, то такой переход должен быть аннулирован – «ЗАПРЕТ НА ЧТЕНИЕ ВВЕРХ» (NRU);
в) если субъект понижает собственный УБП, то требуется ревизия его разрешений на чтение данных в соответствие с новым соотношением УБП и СКД;
г) если субъект повышает собственный УБП, то требуется расширение области разрешенных данных для чтения им;
д) если входной запрос на запись, то он выполняется только когда УБП субъекта не выше, чем СКД объекта, в который осуществляется запись;
е) если входной запрос на запись пытается записать данные в объекты с СКД, ниже чем УБП субъекта, то этот переход должен быть аннулирован – «ЗАПРЕТ НА ЗАПИСЬ ВНИЗ» (NWD);
ж) если субъект понижает собственный УБП, то требуется ревизия его разрешений на запись данных в соответствие с новым соотношением УБП и СКД;
з) если субъект повышает собственный УБП, то требуется сужение области разрешенных данных для записи им.

# ОРГАНИЗАЦИЯ ЗАЩИТЫ БАЗЫ ДАННЫХ

1. Распределить все объекты базы данных по степеням конфиденциальности – присвоить каждому объекту метку конфиденциальности.




2. Распределить все субъекты обработки данных по уровням благонадежности – присвоить каждой учетной записи метку благонадежности.

Ограничить обычных пользователей личными схемами.

```
REVOKE ON SCHEMA public FROM PUBLIC;
```

Удалить схему public из пути поиска по умолчанию для каждого пользователя.

```
ALTER ROLE <имя_учетной_записи> SET search_path = "$user";
```

Пометить каждую учетную запись меткой уровня благонадежности.

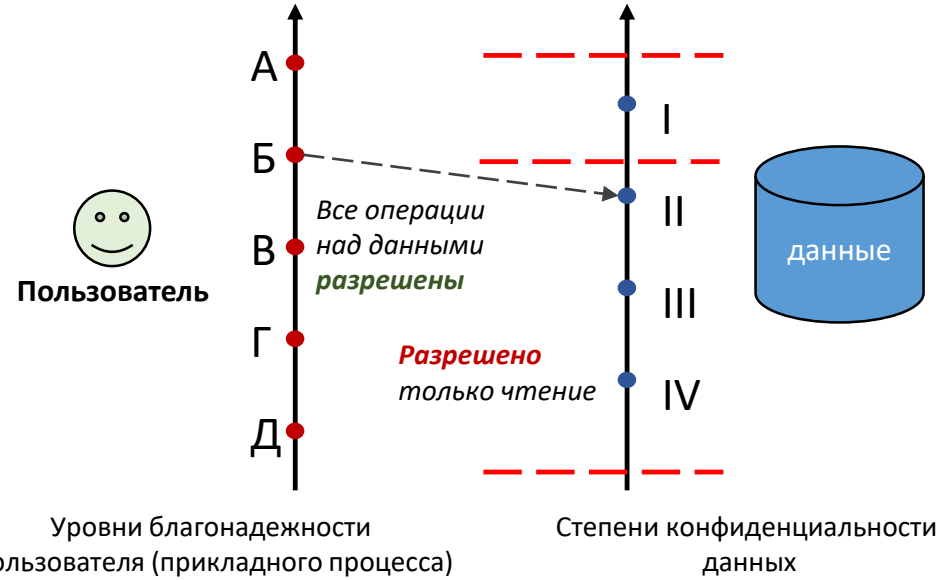
# ОРГАНИЗАЦИЯ ЗАЩИТЫ БАЗЫ ДАННЫХ

3. Определить правило соответствия степеней конфиденциальности данных уровням благонадежности пользователей.

**Дискреционное свойство (discretionary property) механизма защиты** – пользователь имеет полный доступ к данным, когда степень их конфиденциальности соответствует его уровню благонадежности.

**Простое свойство (simple property) механизма защиты** – пользователь имеет право на чтение (`read, select`) данных, когда степень их конфиденциальности ниже или равна его уровню благонадежности.

*** свойство (* property) механизма защиты** – пользователь имеет право на запись (`write, insert, update, delete`) данных, когда степень их конфиденциальности выше или равна его уровню благонадежности.




4. В соответствие с основным свойством концепции сформировать правила назначения полномочий учетным записям пользователей.

```
GRANT SELECT ON <имя_схемы>.<имя_таблицы>,
      INSERT ON <имя_схемы>.<имя_таблицы>,
      UPDATE ON <имя_схемы>.<имя_таблицы>,
      DELETE ON <имя_схемы>.<имя_таблицы>
 TO <имя_учетной_записи>;
```

5. Разработать матрицу безопасности. Присвоить учетным записям пользователей полномочия в соответствие с матрицей безопасности.

## Литература:


1. **Смирнов, С. Н.** Безопасность систем баз данных [Текст]: учеб. пособие для вузов по специальностям в области информационной безопасности. – М.: Гелиос АРВ , 2007. – 350 с.

2. **Федин, Ф. О.** Информационная безопасность баз данных. Ч. 1 [Электронный ресурс]: учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — М.: РТУ МИРЭА, 2020. — Электрон. опт. диск (ISO)

3. **Саймон, А. Р.** Стратегические технологии баз данных: менеджмент на 2000 год: Пер. с англ. /Под ред. и с предисл. М. Р. Когаловского. - М.: Финансы и статистика, 1999 - 479 с.: ил.

4. **Терьо, М.** Oracle. Руководство по безопасности [Текст] / М. Терьо, А. Ньюмен; Пер. с англ.. — М.: Лори, 2004. — 560 с.: ил.

5. **Кузнецов, С. Д.** Основы баз данных: курс лекций : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. ин-форм. технологий / С. Д. Кузнецов. – Москва: Интернет-ун-т ин-форм. технологий, 2005. – 488 с.

6. **Смирнов, С. Н., Задворьев, И. С.** Работаем с ORACLE.: Учебное пособие/2-е изд., испр. и доп. – М: Гелиос АРВ, 2002 г. – 496 с.

7. **Кульба, В.В.** и др. Теоретические основы проектирования оптимальных структур распределенных баз данных. – М: СИНТЕГ, 1999 г. – 660 с.

8. Материалы сервера ORACLE/RE. www.oracle.ru/press/magazine/main.html

9. Материалы информационного ресурса WIKIPEDIA. https://ru.wikipedia.org/wiki/Разграничение_доступа_на_основе_атрибутов; https://ru.wikipedia.org/wiki/Аутентификация; https://ru.wikipedia.org/wiki/Многофакторная_аутентификация; https://ru.wikipedia.org/wiki/Сложность_пароля.

10. Материалы информационного ресурса http://www.nsc.ru/ws/YM2003/6299/